REMARKS

The claims have been amended to more clearly define the invention as disclosed in the written description. In particular, claims 1, 3-6, 8, 9, 11 and 12 have been amended for clarity. Applicant asserts that these changes are editorial and do not affect the scope of the claims.

The Examiner has rejected claims 1-3 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,933,498 to Schneck et al. in view of U.S. Patent 5,864,683 to Boebert et al. The Examiner has further rejected claims 4-7 under 35 U.S.C. 103(a) as being unpatentable over Schneck et al. in view of Boebert et al. In addition, the Examiner has rejected claims 8-13 under 35 U.S.C. 103(a) as being unpatentable over Schneck et al. in view of Boebert et al. Moreover, the Examiner has rejected claims 14-17 under 35 U.S.C. 103(a) as being unpatentable over Schneck et al. in view of Boebert et al. Finally, the Examiner has rejected claims 18-20 under 35 U.S.C. 103(a) as being unpatentable over Schneck et al. in view of Boebert et al.

The Schneck et al. patent discloses a system for controlling access and distribution of digital property, in which, at col. 7, lines 27-33, it is stated that the "invention is a storage device, readable by a machine, tangibly embodying a package of digital data comprising protected portions of digital data, and rules concerning access rights to the digital data whereby a user

is provided controlled access to the digital data only in accordance with the rules as enforced by a tamper detecting access mechanism."

Applicant submits that according to the above, the storage device of Schneck et al. may read on the recording medium of claim 1 having a first memory for storing encrypted content material, and a second memory for storing a secure item (the "rules" of Schneck et al.). However, Applicant has reviewed the section of Schneck et al. identified by the Examiner, to wit, col. 6, line 48 to col. 8, line 58, and nowhere is there any mention of the recording medium containing a recording indicator for containing a unique identifier at each occurrence of a writing of the encrypted content material into the fist memory. Further Schneck et al. neither shows nor suggests that the secure item is based on the unique identifier.

The Boebert et al. patent discloses a system for providing secure internetwork by connecting type enforcing secure computers to external network for limiting access to data based on user and process access rights. The Examiner then indicates that Boebert et al., at col. 6, lines 6-16, discloses a recording indicator including a counter that is configured to be incremented by a recording device when the recording device records the encrypted content material.

Applicant believes that the Examiner is mistaken. In particular, Boebert et al. at col. 6, lines 6-16 states:

> "According to yet another aspect of the present invention, a secure server is described for use in controlling access to data stored within an internal network. The secure server comprises an administrative kernel and an operational kernel, wherein the operational kernel includes security policy program code for enforcing a Type Enforcement security mechanism to restrict access of a process received from the external network to data stored on the internal network and wherein the administrative kernel is restricted to execution only while isolated from the internal network."

Applicant submits that a careful reading of the above section will show that Boebert et al. makes no reference to a recording indicator including a counter that is incremented by a recording device.

Claims 4-7 pertain to a rendering device for rendering (e.g., reproducing) content material contained on a recording medium, in which the recording medium contains encrypted content material and a recording indicator containing an original value. The rendering device includes one or more decrypters for decrypting the encrypted content material based on a current value of the recording indicator, and for providing the decrypted content material only when the current value of the recording indicator corresponds to the original value of the recording indicator.

As noted above with respect to the recording medium, Applicant has reviewed the section of Schneck et al. identified by the Examiner, to wit, col. 6, line 48 to col. 8, line 58, and nowhere is there any mention of the recording medium containing a

recording indicator for containing a unique identifier at each occurrence of a writing of the encrypted content material into the fist memory, and as noted above, Boebert et al. neither shows nor suggest such a recording indicator. Further Schneck et al. neither shows nor suggests that the secure item is based on the unique identifier. As such, Schneck et al., either alone or in combination with Boebert et al., neither shows nor suggests that a rendering device would base its decrypting of the encrypted content material on a current value of the recording indicator, nor does Schneck et al. show or suggest that the provision of the content material is dependent on the current value of the recording indicator corresponding to an original value of the recording indicator.

Claim 5 indicates that the rendering device includes an authorization device for controlling the renderer based on a usage-measure associated with the recording medium, and a validity period associated with the content material. As described in the Substitute Specification on page 4, paragraph [0006], page 5, paragraph [0007], and paragraph [0023] on pages 13-15, a usage-measure pertains to, for example, the number of times a recording medium may be rendered, and a validity period pertains to a time limit during which the content material may be rendered.

Applicant submits that Schneck et al. and/or Boebert et al. neither show nor suggest a rendering device having an

authorization device predicating the rendering of the content material based on such a usage-measure.

Further, since Schneck et al., as noted above, neither shows nor suggests a recording indicator in the recording medium, then surely, Schneck et al. neither shows nor suggests a rendering device having a key generator for creating a unique key based on the current value of the recording indicator, as claimed in claim 6, nor that the decrypters decrypt based on such a unique key.

In the Office Action, the Examiner notes that Schneck et al. does not disclose the subject matter of claim 7, i.e., a first decrypter for decrypting a double encrypted content key, a second decrypter for decrypting the single encrypted content key, and a third decrypter for decrypting the encrypted content material based on the decrypted content key. However, the Examiner alleges that this subject matter is disclosed in Boebert et al. at col. 29, lines 10-35.

Applicant has reviewed this section of Boebert et al. and it discloses a situation where two computer systems are coupled together through a public network, in which the two systems distribute "keys" to each other in a secure manner. In particular:

> "Inbound information flow is essentially symmetric to outbound: the data is received from Public Network 74, if necessary decrypted and has its authentication checked, and then is passed through the Filter Countermeasures 68 to determine whether the organizational security policy allows data of that label, format, or content to be released into Private Network 64. If it does, Secure Computer 48

> uses Local Cryptography to protect and authenticate the transmission to Client Workstation 63. When the Client accesses the data, he or she cain [sic] use that cryptography to verify that the data is what it was authenticated to be over the Public Network 74." (lines 26-37)

It should be apparent to one skilled in the art that Boebert et al. neither discloses nor suggests that a rendering device should include a first decrypter for decrypting a double encrypted content key, a second decrypter for decrypting the single encrypted content key, and a third decrypter for decrypting the encrypted content material based on the decrypted content key.

Claims 8-13 relate to a content material provider which records encrypted content material and a corresponding secure item on a recording medium, in which the content material is encrypted based on a content key, and the secure item is based on a value of a recording indicator of the recording medium.

Again, since, as noted above, neither Schneck et al. nor Boebert et al. disclose a recording medium having a recording indicator, then neither Schneck et al. nor Boebert et al., either individually or collectively, disclose a content material provider which encrypts content material based on a content key, and records this encrypted content material, along with a secure item based on a value of a recording indicator of the recording medium, onto the recording medium.

Claims 14-17 related to a method of providing content material, and are related to the content material provider claims

8-13, while claims 18-20 relate to a method of rendering content material, and are related to the rendering device claims 4-7.

In view of the above, Applicant believe that the subject invention, as claimed, is not rendered obvious by the prior art, either individually or collectively, and as such, is patentable thereover.

Applicant believes that this application, containing claims 1-20, is now in condition for allowance and such action is respectfully requested.

Respectfully submitted,

by _____
Edward W. Goodman, Reg. 28,613
Attorney
Tel.: 914-333-9611

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as First-class mail in an envelope addressed to:

COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

On October 30, 2007

By _____

APPENDIX

1. (Twice amended) A recording medium comprising:

a first memory ~~configured to store~~for storing encrypted content material via a first write operation;

a recording indicator ~~configured to contain~~for containing a unique identifier at each occurrence of the first write operation; and

a second memory ~~configured to store~~for storing, via a second write operation, a secure item based on the unique identifier when the encrypted content material is stored.

3. (Twice amended) The recording medium as claimed in claim 1, wherein:

the recording indicator includes a counter ~~configured to be~~ incremented by a recording device when the recording device records the encrypted content material.

4. (Twice amended) A rendering device ~~configured to render~~for rendering content material corresponding to encrypted content material contained on a recording medium, the recording medium also including a recording indicator ~~that contains~~containing an original value, the rendering device comprising:

one or more decrypters ~~configured to decrypt~~for decrypting the encrypted content material based on a current value of the

recording indicator, said one or more decrypters provide the content material only when the current value of the recording indicator corresponds to the original value of the recording indicator; and

a renderer configured to render the content material.

5. (Twice amended) The rendering device as claimed in claim 4, wherein said rendering device further comprises:

an authorization device ~~configured to control~~for controlling the renderer based on a usage-measure associated with the recording medium, and a validity period associated with the content material.

6. (Twice amended) The rendering device as claimed in claim 4, wherein said rendering device further comprises:

a key generator ~~that creates~~for creating a unique key based on the current value of the recording indicator, and wherein the one or more decrypters ~~are configured to~~ decrypt the encrypted content material based on the unique key based on the current value of the recording indicator.

8. (Twice amended) A provider of content material comprising:

a recorder ~~configured to record~~for recording encrypted content material and a corresponding secure item on a recording medium;

the encrypted content material being encrypted based on a content key; and

the secure item being based on a value of a recording indicator of the recording medium when the encrypted content material is recorded on the recording medium.

9. (Twice amended) The content material provider as claimed in claim 8, wherein the content material provider further comprises:

an allocator ~~configured to allocate~~for allocating rendering rights associated with the encrypted content material, and wherein the recorder ~~is~~ further ~~configured to record~~records the rendering rights on the recording medium.

11. (Twice amended) The content material provider as claimed in claim 8, wherein said content material provider further comprises:

one or more encrypters ~~configured to provide~~for providing the secure item.

12. (Twice amended) The content material provider as claimed in claim 8, wherein said content material provider further comprises:

a key generator for generating a unique key based on the value of the recording indicator; and

one or more encrypters ~~configured to encrypt~~for encrypting the content key based on the unique key to produce the secure item.